

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2017 年 11 月 9 日 (09.11.2017)



(10) 国际公布号
WO 2017/190279 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2016/080928

(22) 国际申请日: 2016 年 5 月 3 日 (03.05.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 应江威(YING, Jiangwei); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 杨艳梅(YANG, Yanmei); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 陈璟(CHEN, Jing); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(CN)。 李琪(LI, Qi); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市海淀区知春路7号致真大厦A1304-05室, Beijing 100191 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(54) Title: CERTIFICATE NOTIFICATION METHOD AND DEVICE

(54) 发明名称: 一种证书通知方法及装置

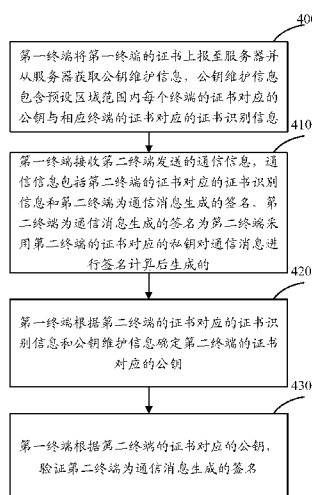


图 4

(57) Abstract: A certificate notification method and device, relating to the technical field of communications and being used for reducing the transmission overhead occupied by certificates and signatures used for security assurance. The method comprises: reporting a certificate of a first terminal to a server and acquiring public key maintenance information from the server; the first terminal receiving communication information sent by a second terminal, wherein the communication information comprises certificate identification information corresponding to a certificate of the second terminal and a signature generated by the second terminal for a communication message; the first terminal determining a public key corresponding to the certificate of the second terminal according to the certificate identification information corresponding to the certificate of the second terminal and the public key maintenance information; and the first terminal verifying the signature generated by the second terminal for the communication message according to the public key corresponding to the certificate of the second terminal. In this way, a communication message sent by a terminal when communicating with other terminals does not need to carry a certificate of the terminal any more, thereby greatly saving the transmission overhead.

(57) 摘要: 一种证书通知方法及装置, 涉及通信技术领域, 用以减少用于安全性保障的证书和签名所占用的传输开销, 该方法为: 第一终端的证书上报至服务器并从服务器获取公钥维护信息; 第一终端接收第二终端发送的通信信息, 通信信息包括第二终端的证书对应的证书识别信息和第二终端为通信消息生成的签名; 第一终端根据第二终端的证书对应的证书识别信息和公钥维护信息确定第二终端的证书对应的公钥; 第一终端根据第二终端的证书对应的公钥, 验证第二终端为通信消息生成的签名。因此, 终端在与其他终端进行通信发送的通信消息中不再需要携带终端的证书, 极大地节省了传输开销。

400 A first terminal reporting a certificate of the first terminal to a server and acquiring public key maintenance information from the server, wherein the public key maintenance information contains a public key corresponding to a certificate of each terminal and certificate identification information about the certificate of the corresponding terminal in a pre-set coverage area.
410 The first terminal receiving communication information sent by a second terminal, wherein the communication information comprises certificate identification information corresponding to a certificate of the second terminal and a signature generated by the second terminal for a communication message.
420 The first terminal determining a public key corresponding to the certificate of the second terminal according to the certificate identification information corresponding to the certificate of the second terminal and the public key maintenance information.
430 The first terminal verifying the signature generated by the second terminal for the communication message according to the public key corresponding to the certificate of the second terminal.

(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则4.17的声明:

- 关于申请人有权申请并被授予专利(细则4.17(ii))

本国际公布:

- 包括国际检索报告(条约第21条(3))。

一种证书通知方法及装置

技术领域

本发明涉及通信技术领域，特别是涉及一种证书通知方法及装置。

背景技术

近年来，汽车网络越来越受到人们的关注，通过车车通信或者车与路边单元之间的通信提高道路交通的安全性、可靠性和交通通行效率。因此，智能交通系统旨在实现车与车、车与人之间、车与路之间的持续通信以交换当前车辆或周围环境状态，减少交通事故、提高交通出行的安全性、帮助缓解交通拥堵、降低能耗、减少污染排放、保护环境、提高运输效率并带动相关产业。

在典型的车联网系统中，采用车车之间的传输，通过车辆之间周期性地交互位置、速度、转向等数据，实现车辆对周围车辆的感知，并利用这些信息实现辅助司机安全驾驶的功能。典型的车联网系统容易部署、低成本、技术成熟，但是其本身也有其缺点：当系统内车辆数目很多时，邻近车辆可能选择同一资源传输数据，因此容易发生资源碰撞，系统性能较差，服务质量（Quality of Service, QoS）不能得到保证，传输距离也比较有限，此外，该系统中需要部署大量路测单元（Road Side Unit, RSU），成本过高。

另外，车辆到车辆（vehicle to vehicle, V2V）通信的安全依赖于公钥基础设施（Public key infrastructure, PKI）证书体系，车车之间传递的V2V消息都要携带证书和签名，带来很大的传输开销。

参阅图1所示，V2V消息的格式如下，其中需要携带证书（Certificate）和签名（Signature）。

参阅图2所示，3GPP的LTE技术具有高速率，低延迟，大覆盖范围，以及支持高速移动终端等优点，可以用于V2V通信，利用中央调度器，例如演进型基站（evolved node B, eNB）实现对车辆进行数据传输所需传输资源的动

态调度，提升了系统性能。

但是，在这种车联网系统中，依旧采用现在欧洲和美国的ITS安全方案来实现车车之间、车与其他设备之间的通信安全（即基于非对称密钥的证书），要求在每条基于LTE的车和其它通信设备之间（Vehicle-to-Everything，LTE-V2X）消息中携带证书和签名。例如，车辆1与车辆2进行通信，车辆1发送第一消息至车辆2，此时，第一消息中需要携带车辆1的证书和车辆1为第一消息生成的签名，该签名是根据车辆1的私钥生成的。车辆2收到第一消息后，根据车辆1的证书导出车辆1的公钥，然后利用车辆1的公钥验证该签名。验证通过后，车辆2解析第一消息中携带的其他内容。

具体的，每条LTE-V2X消息中，证书和签名所占用的传输开销占据LTE-V2X消息本身传输开销的很大比例，因此用于安全性保障的证书和签名所占用的传输开销较大。即使采用现有的优化技术周期性地携带证书来降低传输开销，但是对于LTE-V2X消息来说，安全开销依旧显得过大，不能满足LTE-V2X通信的容量要求。为了保证车辆安全，车车通信的消息需要满足较高的发送频率（比如，10Hz），并需要满足一个eNB覆盖一定数量车辆的容量需求，但车车通信的消息能够使用的空口资源有限（比如，10M），这使得现有的技术方案无法满足上述车联网需求。

发明内容

本发明实施例提供一种证书通知方法及装置，用以减少用于安全性保障的证书和签名所占用的传输开销，尽量满足基于LTE技术实现的车联网系统对车辆通信的容量要求。

本发明实施例提供的具体技术方案如下：

第一方面，一种证书通知方法，包括：第一终端将所述第一终端的证书上报至服务器并从所述服务器获取公钥维护信息，所述公钥维护信息包含预设区域范围内每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息；所述第一终端接收第二终端发送的通信信息，所述通信信息包括所述

第二终端的证书对应的证书识别信息和所述第二终端为所述通信消息生成的签名，所述第二终端为所述通信消息生成的签名为所述第二终端采用所述第二终端的证书对应的私钥对所述通信消息进行签名计算后生成的；所述第一终端根据所述第二终端的证书对应的证书识别信息和所述公钥维护信息确定所述第二终端的证书对应的公钥；所述第一终端根据所述第二终端的证书对应的公钥，验证所述第二终端为所述通信消息生成的签名。

因此，采用本发明实施例提供的方法，终端通过提前获取公钥维护信息，使得在与其他终端进行通信时，不再需要携带该终端的证书，极大地节省了传输开销。

可选地，所述证书识别信息为以下至少一种信息的组合：证书颁发者名称和证书序列号、或者证书名称，或者证书唯一标识。

因此，本发明实施例中证书识别信息可以为多种消息的灵活组合。

可选地，第一终端将所述第一终端的证书上报至服务器，包括：所述第一终端获取到自身的地理位置信息时，将所述地理位置信息和所述第一终端的证书上报至服务器；或者，所述第一终端检测到新的小区全局标识符 ECGI 时，将所述新的 ECGI 和所述第一终端的证书上报至服务器；或者，所述第一终端检测到新的跟踪区域码 TAC 时，将所述新的 TAC 和所述第一终端的证书上报至服务器。

因此，终端上报证书的触发条件可以有多种可能，保证了公钥维护信息能够及时得到更新。

可选地，第一终端将所述第一终端的证书上报至服务器，包括：所述第一终端获取区域配置信息，所述区域配置信息是指以至少一个基站为单位，或以至少一个 TA 为单位，或者根据地理区域进行区域划分的划分结果，每个区域对应一个区域标识；所述第一终端根据所述区域配置信息确定自身所处区域发生变化时，将所述第一终端的证书和所述第一终端所属区域的区域标识发送至服务器。

因此，终端判断自身所处区域发生变化时，可以及时触发上报证书，保

证了公钥维护信息能够及时得到更新。

可选地，所述第一终端根据所述区域配置信息确定自身所处区域发生变化，包括：所述第一终端获取到自身的地理位置信息时，根据所述地理位置信息和所述区域配置信息确定自身所属区域发生变化；或者，所述第一终端检测到新的 ECGI 时，根据所述新的 ECGI 和所述区域配置信息确定自身所属区域发生变化；或者，所述第一终端检测到新的 TAC 时，根据所述新的跟踪区域码 TAC 和所述区域配置信息确定自身所属区域发生变化。

因此，终端可以从多种纬度判断自身所处区域发生变化。

可选地，第一终端将所述第一终端的证书上报至服务器，包括：所述第一终端确定证书更新后需要使用的证书，将所述更新后需要使用的证书上报至所述服务器。

可选地，第一终端从所述服务器获取公钥维护信息，包括：所述第一终端接收所述服务器发送的所述公钥维护信息，或者，所述第一终端接收所述服务器发送的所述第一终端所属区域的区域标识对应的公钥维护消息和所述第一终端所属区域的区域标识。

因此，终端可以通过多种方式获得多种形式的公钥维护信息。

可选地，第一终端从所述服务器获取公钥维护信息，包括：所述第一终端接收所述服务器广播的所述公钥维护消息；或者，所述第一终端接收所述服务器广播的所述第一终端所属区域的区域标识对应的公钥维护消息和所述第一终端所属区域的区域标识。

因此，终端可以通过多种方式获得多种形式的公钥维护信息。

可选地，在第一终端获取公钥维护信息之后，包括：所述第一终端接收公钥维护更新消息，所述公钥维护更新消息用于更新所述第一终端当前存储的公钥维护信息；所述第一终端根据所述公钥维护更新消息更新所述当前存储的公钥维护信息。

因此，终端能够及时更新自身存储的公钥维护信息，保证与其他终端之间的通信畅通。

可选地，所述公钥维护更新消息携带以下至少一种信息的组合：最新公钥维护信息、或者至少一个区域标识和相应区域标识对应的最新公钥维护消息、或者在预设时长内所述公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息以及新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息，或者在预设时长内每个区域标识对应的公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息、新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息和相应的区域标识。

因此，公钥维护更新信息可以采用多种方式灵活组合，广播至各个终端。

第二方面，一种证书通知方法，包括：服务器接收至少一个终端分别上报的相应终端的证书；所述服务器根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息，所述公钥维护信息包含预设区域范围内每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息；所述服务器将所述公钥维护信息通知给所述至少一个终端。

因此，采用本发明实施例提供的方法，服务器获取各个终端的证书，并根据上报的证书更新公钥维护信息并通知给各个终端，使各个终端均能够获取公钥维护信息，保证各个终端间的通信且有效节省了终端间通信的传输开销。

可选地，所述证书识别信息为以下至少一种信息的组合：证书颁发者名称和证书序列号、或者证书名称，或者证书唯一标识。

可选地，所述服务器根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息，包括：所述服务器确定第一终端所属区域发生变化时，根据所述第一终端的证书对应的公钥与所述第一终端的证书对应的证书识别信息更新所述第一终端所属区域的区域标识对应的公钥维护信息，或者，更新所述第一终端所属区域的区域标识对应的公钥维护信息以及至少一个所述第一终端所属区域的相邻区域的区

域标识分别对应的公钥维护信息，所述第一终端为所述至少一个终端中的任意一个终端。

因此，服务器不仅更新了终端所处区域对应的公钥维护信息，还能够针对该区域的各个邻区分别对应的公钥维护信息进行更新，有效保证了各个终端的区域边缘的通信畅通。

可选地，所述服务器确定所述第一终端所属区域发生变化，包括：所述服务器接收所述第一终端上报的所述第一终端所属区域的区域标识；或者，所述服务器获取区域配置信息，根据所述第一终端上报的地理位置信息和所述区域配置信息确定所述第一终端所属区域发生变化；或者，所述服务器获取区域配置信息，根据所述第一终端上报的 ECGI 和所述区域配置信息确定所述第一终端所属区域发生变化；或者，所述服务器获取区域配置信息，根据所述第一终端上报的 TAC 和所述区域配置信息确定所述第一终端所属区域发生变化；其中，所述区域配置信息是指以至少一个基站为单位，或以至少一个 TA 为单位，或根据地理区域进行区域划分的划分结果，每个区域对应一个区域标识。

因此，服务器能够根据终端上报的各种信息，判断终端所处区域是否发生变化。

可选地，所述服务器根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息，包括：所述服务器确定待分析公钥维护信息集合中包含的第一公钥维护信息超时未针对第二终端的证书对应的公钥与所述第二终端的证书对应的证书识别信息进行更新，则所述服务器将所述第二终端的证书对应的公钥与所述第二终端的证书对应的证书识别信息从所述第一公钥维护信息中删除；其中，所述待分析公钥维护信息集合中包含至少一个保存第二终端的证书对应的公钥与所述第二终端的证书对应的证书识别信息的公钥维护信息，所述第一公钥维护信息为所述待分析公钥维护信息集合中的任一条公钥维护信息，所述第二终端为所述至少一个终端中的任意一个终端。

因此，服务器能够将公钥维护信息中的非必要保存的信息的进行删除，节省了传输公钥维护信息的传输开销，保证公钥维护信息的有效性。

可选地，所述服务器根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息，包括：所述服务器确定第三终端从第一区域移动至第二区域时，确定所述第一区域和所述第二区域分别对应的第一邻区集合和第二邻区集合，所述第一邻区集合包含至少一个所述第一区域的相邻区域的区域标识，所述第二邻区集合包含至少一个所述第二区域的相邻区域的区域标识；所述服务器确定所述第一邻区集合与所述第二邻区集合的交集，以及待清理集合，所述待清理集合包含所述第一邻区中非所述交集中包含的区域标识；所述服务器从所述待清理集合中每个区域标识对应的公钥维护信息中，删除所述第三终端的证书对应的公钥与所述第三终端的证书对应的证书识别信息，其中，所述第二终端为所述至少一个终端中的任意一个终端。

因此，服务器能够将公钥维护信息中的非必要保存的信息的进行删除，节省了传输公钥维护信息的传输开销，保证公钥维护信息的有效性。

可选地，所述服务器将所述公钥维护信息通知给所述至少一个终端，包括：所述服务器发送所述公钥维护信息至所述至少一个终端中的每个终端。或者，所述服务器将所述至少一个终端中的每个终端所属区域的区域标识对应的公钥维护信息和相应终端所属区域的区域标识发送至相应的终端。

因此，服务器可以通过多种方式将多种形式的公钥维护信息通知至各个终端。

可选地，所述服务器将所述公钥维护信息通知给所述至少一个终端，包括：所述服务器广播所述公钥维护消息。或者，所述服务器广播至少一个区域标识和相应区域标识对应的公钥维护消息。

因此，服务器可以通过多种方式将多种形式的公钥维护信息通知至各个终端。

可选地，在所述服务器将所述公钥维护信息通知给所述至少一个终端之

后,还包括:所述服务器确定并广播公钥维护更新消息,所述公钥维护更新消息用于更新所述至少一个终端中每个终端当前存储的公钥维护信息;

可选地,所述公钥维护更新消息携带以下至少一种信息的组合:最新公钥维护信息、或者至少一个区域标识和相应区域标识对应的最新公钥维护消息、或者在预设时长内所述公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息以及新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息,或者在预设时长内每个区域标识对应的公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息、新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息和相应的区域标识。

第三方面、一种证书通知装置,包括:上报单元,用于将所述第一终端的证书上报至服务器;获取单元,用于从所述服务器获取公钥维护信息,所述公钥维护信息包含预设区域范围内每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息;接收单元,用于接收第二终端发送的通信信息,所述通信信息包括所述第二终端的证书对应的证书识别信息和所述第二终端为所述通信消息生成的签名,所述第二终端为所述通信消息生成的签名为所述第二终端采用所述第二终端的证书对应的私钥对所述通信消息进行签名计算后生成的;分析单元,用于根据所述第二终端的证书对应的证书识别信息和所述公钥维护信息确定所述第二终端的证书对应的公钥;验证单元,用于根据所述第二终端的证书对应的公钥,验证所述第二终端为所述通信消息生成的签名。

可选地,所述证书识别信息为以下至少一种信息的组合:证书颁发者名称和证书序列号、或者证书名称,或者证书唯一标识。

可选地,将所述第一终端的证书上报至服务器时,所述上报单元,具体用于:所述第一终端获取到自身的地理位置信息时,将所述地理位置信息和所述第一终端的证书上报至服务器;或者,所述第一终端检测到新的小区全局标识符 ECGI 时,将所述新的 ECGI 和所述第一终端的证书上报至服务器;

或者,所述第一终端检测到新的跟踪区域码 TAC 时,将所述新的 TAC 和所述第一终端的证书上报至服务器。

可选地,将所述第一终端的证书上报至服务器时,所述上报单元,具体用于:获取区域配置信息,所述区域配置信息是指以至少一个基站为单位,或以至少一个 TA 为单位,或者根据地理区域进行区域划分的划分结果,每个区域对应一个区域标识;根据所述区域配置信息确定自身所处区域发生变化时,将所述第一终端的证书和所述第一终端所属区域的区域标识发送至服务器。

可选地,根据所述区域配置信息确定自身所处区域发生变化时,所述上报单元,还用于:获取到自身的地理位置信息时,根据所述地理位置信息和所述区域配置信息确定自身所属区域发生变化;或者,检测到新的 ECGI 时,根据所述新的 ECGI 和所述区域配置信息确定自身所属区域发生变化;或者,检测到新的 TAC 时,根据所述新的跟踪区域码 TAC 和所述区域配置信息确定自身所属区域发生变化。

可选地,将所述第一终端的证书上报至服务器,所述上报单元,用于:确定证书更新后需要使用的证书,将所述更新后需要使用的证书上报至所述服务器。

可选地,从所述服务器获取公钥维护信息,所述获取单元,用于:接收所述服务器发送的所述公钥维护信息,或者,接收所述服务器发送的所述第一终端所属区域的区域标识对应的公钥维护消息和所述第一终端所属区域的区域标识。

可选地,从所述服务器获取公钥维护信息,所述获取单元,用于:接收所述服务器广播的所述公钥维护消息;或者,接收所述服务器广播的所述第一终端所属区域的区域标识对应的公钥维护消息和所述第一终端所属区域的区域标识。

可选地,在获取公钥维护信息之后,所述接收单元,还用于所述第一终端接收公钥维护更新消息,所述公钥维护更新消息用于更新所述第一终端当

前存储的公钥维护信息；所述装置还包括：更新单元，根据所述公钥维护更新消息更新所述当前存储的公钥维护信息。

可选地，所述公钥维护更新消息携带以下至少一种信息的组合：最新公钥维护信息、或者至少一个区域标识和相应区域标识对应的最新公钥维护消息、或者在预设时长内所述公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息以及新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息，或者在预设时长内每个区域标识对应的公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息、新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息和相应的区域标识。

第四方面、一种证书通知装置，包括：接收单元，用于接收至少一个终端分别上报的相应终端的证书；维护单元，用于根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息，所述公钥维护信息包含预设区域范围内每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息；发送单元，用于将所述公钥维护信息通知给所述至少一个终端。

可选地，所述证书识别信息为以下至少一种信息的组合：证书颁发者名称和证书序列号、或者证书名称，或者证书唯一标识。

可选地，根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息时，所述维护单元，具体用于包括：确定第一终端所属区域发生变化时，根据所述第一终端的证书对应的公钥与所述第一终端的证书对应的证书识别信息更新所述第一终端所属区域的区域标识对应的公钥维护信息，或者，更新所述第一终端所属区域的区域标识对应的公钥维护信息以及至少一个所述第一终端所属区域的相邻区域的区域标识分别对应的公钥维护信息，所述第一终端为所述至少一个终端中的任意一个终端。

可选地，确定所述第一终端所属区域发生变化时，所述维护单元，还用

于：接收所述第一终端上报的所述第一终端所属区域的区域标识；或者，获取区域配置信息，根据所述第一终端上报的地理位置信息和所述区域配置信息确定所述第一终端所属区域发生变化；或者，获取区域配置信息，根据所述第一终端上报的 ECGI 和所述区域配置信息确定所述第一终端所属区域发生变化；或者，获取区域配置信息，根据所述第一终端上报的 TAC 和所述区域配置信息确定所述第一终端所属区域发生变化；其中，所述区域配置信息是指以至少一个基站为单位，或以至少一个 TA 为单位，或根据地理区域进行区域划分的划分结果，每个区域对应一个区域标识。

可选地，根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息，所述维护单元，还用于：确定待分析公钥维护信息集合中包含的第一公钥维护信息超时未针对第二终端的证书对应的公钥与所述第二终端的证书对应的证书识别信息进行更新，则所述服务器将所述第二终端的证书对应的公钥与所述第二终端的证书对应的证书识别信息从所述第一公钥维护信息中删除；其中，所述待分析公钥维护信息集合中包含至少一个保存第二终端的证书对应的公钥与所述第二终端的证书对应的证书识别信息的公钥维护信息，所述第一公钥维护信息为所述待分析公钥维护信息集合中的任一条公钥维护信息，所述第二终端为所述至少一个终端中的任意一个终端。

可选地，根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息，所述维护单元，还用于：确定第三终端从第一区域移动至第二区域时，确定所述第一区域和所述第二区域分别对应的第一邻区集合和第二邻区集合，所述第一邻区集合包含至少一个所述第一区域的相邻区域的区域标识，所述第二邻区集合包含至少一个所述第二区域的相邻区域的区域标识；确定所述第一邻区集合与所述第二邻区集合的交集，以及待清理集合，所述待清理集合包含所述第一邻区中非所述交集中包含的区域标识；从所述待清理集合中每个区域标识对应的公钥维护信息中，删除所述第三终端的证书对应的公钥与所述第三终端的证书对应

的证书识别信息，其中，所述第二终端为所述至少一个终端中的任意一个终端。

可选地，将所述公钥维护信息通知给所述至少一个终端时，所述发送单元，具体用于：发送所述公钥维护信息至所述至少一个终端中的每个终端。或者，将所述至少一个终端中的每个终端所属区域的区域标识对应的公钥维护信息和相应终端所属区域的区域标识发送至相应的终端。

可选地，将所述公钥维护信息通知给所述至少一个终端时，所述发送单元，具体用于：广播所述公钥维护消息。或者，广播至少一个区域标识和相应区域标识对应的公钥维护消息。

可选地，在将所述公钥维护信息通知给所述至少一个终端之后，所述发送单元还用于：确定并广播公钥维护更新消息，所述公钥维护更新消息用于更新所述至少一个终端中每个终端当前存储的公钥维护信息；

可选地，所述公钥维护更新消息携带以下至少一种信息的组合：最新公钥维护信息、或者至少一个区域标识和相应区域标识对应的最新公钥维护消息、或者在预设时长内所述公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息以及新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息，或者在预设时长内每个区域标识对应的公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息、新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息和相应的区域标识。

第五方面，本发明实施例提供一种终端，包括收发器、处理器和存储器，收发器、处理器以及存储器之间通过总线连接，其中：收发器，用于将第一终端的证书上报至服务器并从服务器获取公钥维护信息，以及接收第二终端发送的通信信息，通信信息包括第二终端的证书对应的证书识别信息和第二终端为通信消息生成的签名，第二终端为通信消息生成的签名为第二终端采用第二终端的证书对应的私钥对通信消息进行签名计算后生成的。存储器，用于存储处理器执行的程序代码。处理器，用于通过存储器中的程序代码，

执行以下操作：根据第二终端的证书对应的证书识别信息和公钥维护信息确定第二终端的证书对应的公钥，以及根据第二终端的证书对应的公钥，验证第二终端为通信消息生成的签名。

第六方面，本发明实施例提供一种服务器，包括收发器、处理器和存储器，收发器、处理器以及存储器之间通过总线连接，其中：收发器，用于接收至少一个终端分别上报的相应终端的证书，以及将公钥维护信息通知给至少一个终端。存储器，用于存储处理器执行的程序代码。处理器，用于通过存储器中的程序代码，执行以下操作：根据至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息，公钥维护信息包含预设区域范围内每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息。

本发明实施例中第一终端的证书上报至服务器并从服务器获取公钥维护信息，使得第一终端在与其他终端进行通信之前及时获取公钥维护信息；第一终端接收第二终端发送的通信信息，通信信息包括第二终端的证书对应的证书识别信息和第二终端为通信消息生成的签名，此时通信消息中不再需要携带第一终端的证书，极大地节省了传输开销；第一终端根据第二终端的证书对应的证书识别信息和公钥维护信息确定第二终端的证书对应的公钥；第一终端根据第二终端的证书对应的公钥，验证第二终端为通信消息生成的签名。服务器接收至少一个终端分别上报的相应终端的证书；服务器根据至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息；服务器将公钥维护信息通知给至少一个终端，使各个终端均能够获取公钥维护信息，保证各个终端间的通信且有效节省了终端间通信的传输开销。

附图说明

图1为本发明背景技术中V2V消息的格式示意图；

图2为本发明实施例中基于LTE的车和其它通信设备的车联网结构示意图；

- 图3为本发明实施例中LTE-V2X通信系统的结构示意图；
- 图4为本发明实施例中终端侧证书通知方法的概述流程图；
- 图5为本发明实施例中终端所处区域划分的结构示意图；
- 图6为本发明实施例中服务器侧证书通知方法的概述流程图；
- 图7为本发明实施例中终端所处区域发生变化的示意图；
- 图8为本发明实施例中证书通知方法的具体流程图之一；
- 图9为本发明实施例中证书通知方法的具体流程图之二；
- 图10为本发明实施例中终端侧对应的证书通知装置结构示意图；
- 图11为本发明实施例中服务器侧对应的证书通知装置结构示意图；
- 图12为本发明实施例中一种终端的结构示意图；
- 图13为本发明实施例中一种服务器的结构示意图。

具体实施方式

本发明实施例提供一种证书通知方法及装置，用以减少用于安全性保障的证书和签名所占用的传输开销，尽量满足基于LTE技术实现的车联网系统对车辆通信的容量要求。

其中，方法、装置是基于同一发明构思的，由于方法、装置解决问题的原理相似，因此装置与方法的实施可以相互参见，重复之处不再赘述。

本发明实施例的主要应用场景为参阅图3所示的LTE-V2X通信系统。该系统中包括证书的权威机构(CA)，eNB，以及各种车辆和其他通信设备(例如车辆1、车辆2、车辆3)，服务器，例如移动边缘计算实体(Mobile edge computing, MEC)或路侧单元(Road Side Unit, RSU)或密钥管理服务(KeyManagementService, KMS)或LTE-V2X Server，其中，服务器可以不在运营商域内。

具体的，CA为服务器、车辆1、车辆2、车辆3分别颁发证书。

参阅图4所示，本发明实施例提供一种证书通知方法，包括：

步骤400：第一终端将第一终端的证书上报至服务器并从服务器获取公钥

维护信息，公钥维护信息包含预设区域范围内每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息。

可选地，证书识别信息为以下至少一种信息的组合：证书颁发者名称和证书序列号、或者证书名称，或者证书唯一标识。

一般地，证书识别信息为证书颁发者名称和证书序列号，利用证书颁发者名称和证书序列号来唯一标识一张证书。

步骤 410: 第一终端接收第二终端发送的通信信息，通信信息包括第二终端的证书对应的证书识别信息和第二终端为通信消息生成的签名，第二终端为通信消息生成的签名为第二终端采用第二终端的证书对应的私钥对通信信息进行签名计算后生成的。

因此，第一终端只需携带第一终端为所要发送的信息生成的签名和第一终端的证书对应的证书识别信息，而无需再携带第一终端的证书，极大地减少了传输开销。

和专用短程通信技术（Dedicated Short Range Communications, DSRC）证书方案比，本发明实施例提供的方案省去了 PC5 口 LTE-V2X 消息中需要携带证书的安全开销，大概 117Bytes 左右（而 LTE-V2X 消息典型值为 50~100Bytes），因此可以明显减少 PC5 口上消息的安全开销，提高了 LTE-V2X 的系统容量。

步骤 420: 第一终端根据第二终端的证书对应的证书识别信息和公钥维护信息确定第二终端的证书对应的公钥；

步骤 430: 第一终端根据第二终端的证书对应的公钥，验证第二终端为通信消息生成的签名。

在执行步骤 400 时，第一终端将第一终端的证书上报至服务器，与第一终端从服务器获取公钥维护信息，两个过程没有先后顺序。

第一终端将第一终端的证书上报至服务器，可以采用但不限于以下几种方式：

第一种方式：第一终端获取到自身的地理位置信息时，将地理位置信息

和第一终端的证书上报至服务器。

例如,第一终端通过自身全球定位系统(Global Positioning System, GPS)等获取自身的地理位置信息。

服务器获取区域配置信息,根据第一终端上报的地理位置信息和区域配置信息确定第一终端所属区域发生变化时,根据第一终端的证书对应的公钥与第一终端的证书对应的证书识别信息更新公钥维护信息。

这里的区域配置信息是指以至少一个基站为单位,或以至少一个跟踪区(Tracking Area, TA)为单位,或根据地理区域进行区域划分的划分结果,每个区域对应一个区域标识。该区域配置信息可以由服务器事先进行配置,并可将该区域配置信息下发至服务区所辖区域内的各个终端。

第二种方式:第一终端检测到新的小区 ECGI 时,将新的 ECGI 和第一终端的证书上报至服务器。

其中,小区全局标识符(E-UTRAN cell global identifier, ECGI)用于全局标识一个小区,ECGI 就是由 PLMN Identifier 和 E-UTRAN Cell Identifier 组成。

服务器获取区域配置信息,根据第一终端上报的 ECGI 和区域配置信息确定第一终端所属区域发生变化时,根据第一终端的证书对应的公钥与第一终端的证书对应的证书识别信息更新公钥维护信息。

第三种方式:第一终端检测到新的跟踪区域码(Tracking Area Code, TAC)时,将新的 TAC 和第一终端的证书上报至服务器。

服务器获取区域配置信息,根据第一终端上报的 TAC 和区域配置信息确定第一终端所属区域发生变化时,根据第一终端的证书对应的公钥与第一终端的证书对应的证书识别信息更新公钥维护信息。

此外,还可以由第一终端根据区域配置信息,事先判断自身所属区域是否发生变化。

可选地,对应上述三种方式,第一终端确定自身所属区域发生变化,也可以有三种方式:

(1)第一终端获取到自身的地理位置信息时,根据地理位置信息和区域

配置信息确定自身所属区域发生变化。

(2) 第一终端检测到新的 ECGI 时, 根据新的 ECGI 和区域配置信息确定自身所属区域发生变化。

(3) 第一终端检测到新的 TAC 时, 根据新的 TAC 和区域配置信息确定自身所属区域发生变化。

第四种方式, 针对上述三种确定第一终端所属区域发生变化的方式或者其他可能的实现方式, 第一终端确定自身所属区域发生变化时, 将第一终端的证书和第一终端所属区域的区域标识发送至服务器。

可选地, 服务器根据第一终端的证书对应的公钥与第一终端的证书对应的证书识别信息更新第一终端所属区域的区域标识对应的公钥维护信息, 或者, 更新第一终端所属区域的区域标识对应的公钥维护信息以及至少一个第一终端所属区域的相邻区域的区域标识分别对应的公钥维护信息。

例如, 参阅图 5 所示, 图中所示的各个长方形为事先划分的区域, 每个长方形代表一个区域, 假设第一终端当前所属区域为 5, 则根据第一终端的证书对应的公钥与第一终端的证书对应的证书识别信息更新区域 5 对应的公钥维护信息, 或者, 区域 1~区域 9 分别对应的公钥维护信息。此时, 区域 1~区域 9 (除区域 5) 为区域 5 的邻区。

第五种方式, 第一终端确定证书更新后需要使用的证书, 将更新后需要使用的证书上报至服务器。

例如, 第一终端可能每 10 分钟更新一次证书。

服务器根据第一终端的证书对应的公钥与第一终端的证书对应的证书识别信息更新公钥维护信息。

此外, 针对上述五种第一终端将第一终端的证书上报至服务器的方式, 在第一终端上报第一终端的证书时还需携带第一终端为这次上报的消息生成的签名。

服务器收到该消息后, 验证证书的合法性并且根据第一终端的证书中包含的公钥验证该签名, 验证通过后, 根据第一终端的证书导出第一终端的公

钥和证书识别信息，用于更新公钥维护信息。

在执行步骤 400 时，第一终端从服务器获取公钥维护信息，可以采用但不限于几种方式：

第一种方式：第一终端接收服务器发送的公钥维护信息，

这里的公钥维护信息是服务器直接发送给终端的，该公钥维护信息可以包括服务器所辖范围内的每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息。

第二种方式：第一终端接收服务器发送的第一终端所属区域的区域标识对应的公钥维护消息和第一终端所属区域的区域标识。

这里的公钥维护信息是服务器直接发送给终端的，该公钥维护信息可以包括第一终端所属区域内的每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息。

第三种方式：第一终端接收服务器广播的公钥维护消息。

例如，服务器可以通过 eNB 在每次做多媒体广播多播业务（Multimedia Broadcast Multicast Service, MBMS）广播时广播公钥维护消息，该公钥维护消息可以为服务器所辖范围内的每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息。

第四种方式：第一终端接收服务器广播的第一终端所属区域的区域标识对应的公钥维护消息和第一终端所属区域的区域标识。

即服务器可以每次广播至少一个区域标识和相应区域标识对应的公钥维护消息。

针对上述四种第一终端获取公钥维护信息的方式，可以发生在第一终端上报第一终端的证书之前或之后，也可以是上述四种方式中至少一种方式的组合。此外，在第一终端收到的包含公钥维护信息和/或第一终端所属区域的区域标识对应的公钥维护消息和第一终端所属区域的区域标识的消息中，还需携带服务器的证书和服务器的本次通知消息（单播方式或多播方式）生成的签名。

第一终端收到该通知消息后，验证服务器的证书的合法性并且根据服务器的证书中包含的公钥验证该签名，验证通过后，存储该通知消息中携带的公钥维护信息和/或第一终端所属区域的区域标识对应的公钥维护消息和第一终端所属区域的区域标识。

进一步地，在第一终端获取公钥维护信息之后，需要对当前存储的公钥维护信息进行更新。第一终端接收公钥维护更新消息，公钥维护更新消息用于更新第一终端当前存储的公钥维护信息，第一终端根据公钥维护更新消息更新当前存储的公钥维护信息。

具体的，公钥维护更新消息携带以下至少一种信息的组合：最新公钥维护信息、或者至少一个区域标识和相应区域标识对应的最新公钥维护消息、或者在预设时长内公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息以及新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息，或者在预设时长内每个区域标识对应的公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息、新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息和相应的区域标识。

例如，在终端 1 获得公钥维护信息后，终端 2 和终端 3 将分别对应的证书上报至服务器，服务器广播最新的公钥维护信息，最新的公钥维护信息中新增了终端 2 的证书对应的公钥与终端 2 的证书对应的证书识别信息，以及终端 3 的证书对应的公钥与终端 3 的证书对应的证书识别信息，终端 1 收到该广播消息后，采用最新的公钥维护信息替换当前存储的公钥维护信息；

或者，服务器只将终端 2 的证书对应的公钥与终端 2 的证书对应的证书识别信息，以及终端 3 的证书对应的公钥与终端 3 的证书对应的证书识别信息携带在广播消息中进行广播，终端 1 收到后，利用广播消息对当前存储的公钥维护信息进行更新。

参阅图 6 所示，本发明实施例提供一种证书通知方法，包括：

步骤 600：服务器接收至少一个终端分别上报的相应终端的证书。

步骤 610: 服务器根据至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息, 公钥维护信息包含预设区域范围内每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息。

步骤 620: 服务器将公钥维护信息通知给至少一个终端。

其中, 步骤 600 和步骤 620 分别与上述第一终端将第一终端的证书上报至服务器和第一终端从服务器获取公钥维护信息相对应, 此处不再赘述。

在执行步骤 610 时, 除了将新上报的终端的证书对应的公钥和相应终端的证书对应的证书识别信息新增至公钥维护信息, 以及证书的定时更新时采用终端的最新证书对应的公钥和相应终端的最新证书对应的证书识别信息替换在公钥维护信息中相应终端原来保存的信息, 还需对公钥维护信息中的不必要保存的信息进行删除, 这里可以采用但不限于以下两种方式:

第一种方式: 服务器确定待分析公钥维护信息集合中包含的第一公钥维护信息超时未针对第二终端的证书对应的公钥与第二终端的证书对应的证书识别信息进行更新, 则服务器将第二终端的证书对应的公钥与第二终端的证书对应的证书识别信息从第一公钥维护信息中删除。

其中, 待分析公钥维护信息集合中包含至少一个保存第二终端的证书对应的公钥与第二终端的证书对应的证书识别信息的公钥维护信息, 第一公钥维护信息为待分析公钥维护信息集合中的任一条公钥维护信息, 第二终端为至少一个终端中的任意一个终端。

参阅图 7 所示, 当终端 1 在区域 5 中时, 区域 1~区域 9 分别对应的公钥维护信息均包含终端 1 的证书对应的公钥与终端 1 的证书对应的证书识别信息。终端 1 对应的待分析公钥维护信息集合包括区域 1~区域 9 分别对应的公钥维护信息, 并针对其中每个区域对应的公钥维护信息设置定时器。终端 1 从区域 5 移动至区域 7 时, 区域 4、区域 5、区域 7、区域 8 分别对应的公钥维护信息的定时器清零并重新计时, 因为, 区域 4、区域 5、区域 8 为区域 7 的邻区。而区域 1、区域 2、区域 3、区域 6、区域 9 的定时器则继续计时,

当定时器超时时，终端 1 的证书对应的公钥与终端 1 的证书对应的证书识别信息依旧没有进行更新，因此将终端 1 的证书对应的公钥与终端 1 的证书对应的证书识别信息从区域 1、区域 2、区域 3、区域 6、区域 9 分别对应的公钥维护信息中删除。

第二种方式：服务器确定第三终端从第一区域移动至第二区域时，确定第一区域和第二区域分别对应的第一区域集合和第二区域集合，第一邻区集合包含至少一个第一区域的相邻区域的区域标识和第一区域的区域标识，第二区域集合包含至少一个第二区域的相邻区域的区域标识和第二区域的区域标识；

服务器确定第一区域集合与第二区域集合的交集，以及待清理集合，待清理集合包含第一区域中非交集中包含的区域标识；

服务器从待清理集合中每个区域标识对应的公钥维护信息中，删除第三终端的证书对应的公钥与第三终端的证书对应的证书识别信息，其中，第二终端为至少一个终端中的任意一个终端。

参阅图 7 所示，当终端 1 从区域 5 移动至区域 7 时，确定区域 5 对应的区域集合（区域 1、区域 2、区域 3、区域 4、区域 5、区域 6、区域 7、区域 8、区域 9），以及区域 7 对应的邻区集合（区域 4、区域 5、区域 7、区域 8、区域 10、区域 11、区域 12、区域 13、区域 14），进一步地根据区域 5 对应的区域集合和区域 7 对应的区域集合，确定两者的交集为区域 4、区域 5、区域 7、区域 8，区域 5 对应的区域集合中非该交集中包含的区域为待清理集合（区域 1、区域 2、区域 3、区域 6、区域 9），因此将终端 1 的证书对应的公钥与终端 1 的证书对应的证书识别信息从区域 1、区域 2、区域 3、区域 6、区域 9 分别对应的公钥维护信息中删除。

参阅图 8 所示，本发明实施例提供一种证书通知方法，其具体流程为：

S801: 车辆 1 检测到自身的地理位置信息，确定自身所属区域发生变化。

例如，车辆 1 从区域 2 移动至区域 1。

在车辆 1 检测到自身的地理位置信息，确定自身所属区域发生变化之前，

还需执行以下操作:

CA 已经为车辆 1、车辆 2 和 LTE-V2X Server 或 KMS 分别颁发证书。

车辆 1 与 PDN 网关 (PDN GateWay, PGW) 之间已经成功建立公用数据网 (Public Data Network, PDN) 连接。

LTE-V2X Server 或 KMS 对 V2X 区域进行划分, 得到每个区域对应的区域标识, 以及每个区域对应的区域标识与广播和多播业务中心 (broadcast and multicast service center, BM-SC) 管理的各个基站的基站标识的对应关系, 作为区域配置信息。

S802: 车辆 1 上报证书通知消息, 该证书通知消息中携带车辆 1 所属区域 1 的区域标识, 车辆 1 的证书以及车辆 1 为该证书通知消息生成的签名。

S803: LTE-V2X Server 或 KMS 验证车辆 1 的证书的合法性, 并根据车辆 1 的证书中包含的公钥验证车辆 1 为该证书通知消息生成的签名, 验证通过后将终端 1 的证书对应的公钥与终端 1 的证书对应的证书识别信息存入区域 1 对应的公钥维护信息中。

S804: LTE-V2X Server 或 KMS 发送证书通知确认消息至车辆 1, 该证书通知确认消息中携带 LTE-V2X Server 或 KMS 的证书、LTE-V2X Server 或 KMS 为该证书通知确认消息生成的签名、区域 1 的区域标识以及区域 1 对应的公钥维护信息。

S805: 车辆 1 验证 LTE-V2X Server 或 KMS 的证书的合法性, 并根据 LTE-V2X Server 或 KMS 的证书中的公钥验证 LTE-V2X Server 或 KMS 为该证书通知确认消息生成的签名, 验证通过后保存区域 1 的区域标识以及区域 1 对应的公钥维护信息。

S806: LTE-V2X Server 或 KMS 将公钥通知消息发送给 BM-SC, 该公钥通知消息中携带 LTE-V2X Server 或 KMS 的证书、LTE-V2X Server 或 KMS 为该公钥通知消息生成的签名、区域 1 的区域标识以及区域 1 对应的公钥维护信息。

S807: BM-SC 广播该公钥通知消息。

S808: 车辆 1 (车辆 2) 接收该公钥通知消息, 验证 LTE-V2X Server 或 KMS 的证书的合法性, 并根据 LTE-V2X Server 或 KMS 的证书中的公钥验证 LTE-V2X Server 或 KMS 为该公钥通知消息生成的签名, 验证通过后更新区域 1 对应的公钥维护信息。

S809: 车辆 2 向车辆 1 发送的通信信息, 通信信息包括车辆 2 的证书对应的证书识别信息和车辆 2 为通信消息生成的签名。

S810: 车辆 1 根据车辆 2 的证书对应的证书识别信息和区域 1 对应的公钥维护信息确定车辆 2 的证书对应的公钥。车辆 1 根据车辆 2 的证书对应的公钥, 验证车辆 2 为通信消息生成的签名。

上述实施例中, 车辆 1 可以通过两种方式获得公钥维护信息, 即 S804~S805 (由 LTE-V2X Server 或 KMS 发送证书通知确认消息给车辆 1) 和 S806~S808 (由 LTE-V2X Server 或 KMS 通过 BM-SC 广播公钥通知消息), 因此, S804~S805 为可选的实施方式。

参阅图 9 所示, 本发明实施例提供一种证书通知方法, 其具体流程为:

S901~S905 与图 8 中的 S801~S805 相同。在本实施例中, S904~S905 为必须执行的步骤。

S906: LTE-V2X Server 或 KMS 将公钥通知消息发送给 BM-SC, 该公钥通知消息中携带 LTE-V2X Server 或 KMS 的证书、LTE-V2X Server 或 KMS 为该公钥通知消息生成的签名、区域 1 的区域标识以及在预设时长内区域 1 对应的公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息、新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息。

S907: BM-SC 广播该公钥通知消息。

S908: 车辆 1 (车辆 2) 接收该公钥通知消息, 验证 LTE-V2X Server 或 KMS 的证书的合法性, 并根据 LTE-V2X Server 或 KMS 的证书中的公钥验证 LTE-V2X Server 或 KMS 为该公钥通知消息生成的签名, 验证通过后更新区域 1 对应的公钥维护信息。

参阅图 10 所示, 本发明实施例提供一种证书通知装置 1000, 包括:

上报单元 1010, 用于将第一终端的证书上报至服务器;

获取单元 1020, 用于从服务器获取公钥维护信息, 公钥维护信息包含预设区域范围内每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息;

接收单元 1030, 用于接收第二终端发送的通信信息, 通信信息包括第二终端的证书对应的证书识别信息和第二终端为通信消息生成的签名, 第二终端为通信消息生成的签名为第二终端采用第二终端的证书对应的私钥对通信消息进行签名计算后生成的;

分析单元 1040, 用于根据第二终端的证书对应的证书识别信息和公钥维护信息确定第二终端的证书对应的公钥;

验证单元 1050, 用于根据第二终端的证书对应的公钥, 验证第二终端为通信消息生成的签名。

可选地, 证书识别信息为以下至少一种信息的组合: 证书颁发者名称和证书序列号、或者证书名称, 或者证书唯一标识。

可选地, 将第一终端的证书上报至服务器时, 上报单元 1010, 具体用于:

第一终端获取到自身的地理位置信息时, 将地理位置信息和第一终端的证书上报至服务器;

或者, 第一终端检测到新的小区全局标识符 ECGI 时, 将新的 ECGI 和第一终端的证书上报至服务器;

或者, 第一终端检测到新的跟踪区域码 TAC 时, 将新的 TAC 和第一终端的证书上报至服务器。

可选地, 将第一终端的证书上报至服务器时, 上报单元 1010, 具体用于:

获取区域配置信息, 区域配置信息是指以至少一个基站为单位, 或以至少一个 TA 为单位, 或者根据地理区域进行区域划分的划分结果, 每个区域对应一个区域标识;

根据区域配置信息确定自身所处区域发生变化时, 将第一终端的证书和

第一终端所属区域的区域标识发送至服务器。

可选地,根据区域配置信息确定自身所处区域发生变化时,上报单元 1010,还用于:

获取到自身的地理位置信息时,根据地理位置信息和区域配置信息确定自身所属区域发生变化;

或者,检测到新的 ECGI 时,根据新的 ECGI 和区域配置信息确定自身所属区域发生变化;

或者,检测到新的 TAC 时,根据新的跟踪区域码 TAC 和区域配置信息确定自身所属区域发生变化。

可选地,将第一终端的证书上报至服务器,上报单元 1010,用于:

确定证书更新后需要使用的证书,将更新后需要使用的证书上报至服务器。

可选地,从服务器获取公钥维护信息,获取单元 1020,用于:

接收服务器发送的公钥维护信息,

或者,接收服务器发送的第一终端所属区域的区域标识对应的公钥维护消息和第一终端所属区域的区域标识。

可选地,从服务器获取公钥维护信息,获取单元 1020,用于:

接收服务器广播的公钥维护消息。

或者,接收服务器广播的第一终端所属区域的区域标识对应的公钥维护消息和第一终端所属区域的区域标识。

可选地,在获取公钥维护信息之后,接收单元 1030,还用于第一终端接收公钥维护更新消息,公钥维护更新消息用于更新第一终端当前存储的公钥维护信息;

装置还包括:

更新单元 1060,根据公钥维护更新消息更新当前存储的公钥维护信息。

可选地,公钥维护更新消息携带以下至少一种信息的组合:最新公钥维护信息、或者至少一个区域标识和相应区域标识对应的最新公钥维护消息、

或者在预设时长内公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息以及新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息，或者在预设时长内每个区域标识对应的公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息、新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息和相应的区域标识。

参阅图 11 所示，本发明实施例提供一种证书通知装置 1100，包括：

接收单元 1110，用于接收至少一个终端分别上报的相应终端的证书；

维护单元 1120，用于根据至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息，公钥维护信息包含预设区域范围内每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息；

发送单元 1130，用于将公钥维护信息通知给至少一个终端。

可选地，证书识别信息为以下至少一种信息的组合：证书颁发者名称和证书序列号、或者证书名称，或者证书唯一标识。

可选地，根据至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息时，维护单元 1120，具体用于包括：

确定第一终端所属区域发生变化时，根据第一终端的证书对应的公钥与第一终端的证书对应的证书识别信息更新第一终端所属区域的区域标识对应的公钥维护信息，或者，更新第一终端所属区域的区域标识对应的公钥维护信息以及至少一个第一终端所属区域的相邻区域的区域标识分别对应的公钥维护信息，第一终端为至少一个终端中的任意一个终端。

可选地，确定第一终端所属区域发生变化时，维护单元 1120，还用于：

接收第一终端上报的第一终端所属区域的区域标识；

或者，获取区域配置信息，根据第一终端上报的地理位置信息和区域配置信息确定第一终端所属区域发生变化；

或者, 获取区域配置信息, 根据第一终端上报的 ECGI 和区域配置信息确定第一终端所属区域发生变化;

或者, 获取区域配置信息, 根据第一终端上报的 TAC 和区域配置信息确定第一终端所属区域发生变化;

其中, 区域配置信息是指以至少一个基站为单位, 或以至少一个 TA 为单位, 或根据地理区域进行区域划分的划分结果, 每个区域对应一个区域标识。

可选地, 根据至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息, 维护单元 1120, 还用于:

确定待分析公钥维护信息集合中包含的第一公钥维护信息超时未针对第二终端的证书对应的公钥与第二终端的证书对应的证书识别信息进行更新, 则服务器将第二终端的证书对应的公钥与第二终端的证书对应的证书识别信息从第一公钥维护信息中删除;

其中, 待分析公钥维护信息集合中包含至少一个保存第二终端的证书对应的公钥与第二终端的证书对应的证书识别信息的公钥维护信息, 第一公钥维护信息为待分析公钥维护信息集合中的任一条公钥维护信息, 第二终端为至少一个终端中的任意一个终端。

可选地, 根据至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息, 维护单元 1120, 还用于:

确定第三终端从第一区域移动至第二区域时, 确定第一区域和第二区域分别对应的第一邻区集合和第二邻区集合, 第一邻区集合包含至少一个第一区域的相邻区域的区域标识, 第二邻区集合包含至少一个第二区域的相邻区域的区域标识;

确定第一邻区集合与第二邻区集合的交集, 以及待清理集合, 待清理集合包含第一邻区中非交集中包含的区域标识;

从待清理集合中每个区域标识对应的公钥维护信息中, 删除第三终端的证书对应的公钥与第三终端的证书对应的证书识别信息, 其中, 第二终端为至少一个终端中的任意一个终端。

可选地，将公钥维护信息通知给至少一个终端时，发送单元 1130，具体用于：

发送公钥维护信息至至少一个终端中的每个终端。或者，将至少一个终端中的每个终端所属区域的区域标识对应的公钥维护信息和相应终端所属区域的区域标识发送至相应的终端。

可选地，将公钥维护信息通知给至少一个终端时，发送单元 1130，具体用于：

广播公钥维护消息。

或者，广播至少一个区域标识和相应区域标识对应的公钥维护消息。

可选地，在将公钥维护信息通知给至少一个终端之后，发送单元 1130 还用于：

确定并广播公钥维护更新消息，公钥维护更新消息用于更新至少一个终端中每个终端当前存储的公钥维护信息；

可选地，公钥维护更新消息携带以下至少一种信息的组合：最新公钥维护信息、或者至少一个区域标识和相应区域标识对应的最新公钥维护消息、或者在预设时长内公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息以及新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息，或者在预设时长内每个区域标识对应的公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息、新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息和相应的区域标识。

需要说明的是，本发明实施例中对模块的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，另外，在本申请各个实施例中的各功能模块可以集成在一个处理模块中，也可以是各个模块单独物理存在，也可以两个或两个以上模块集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。

集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使

用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本申请各个实施例方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

参阅图 12 所示，本发明实施例提供一种终端 1200，包括收发器 1201、处理器 1202 和存储器 1203，收发器 1201、处理器 1202 以及存储器 1203 之间通过总线 1204 连接，其中：

收发器 1201，用于将第一终端的证书上报至服务器并从服务器获取公钥维护信息，以及接收第二终端发送的通信信息，通信信息包括第二终端的证书对应的证书识别信息和第二终端为通信消息生成的签名，第二终端为通信消息生成的签名为第二终端采用第二终端的证书对应的私钥对通信消息进行签名计算后生成的。

存储器 1203，用于存储处理器 1202 执行的程序代码。

处理器 1202，用于通过存储器 1203 中的程序代码，执行以下操作：根据第二终端的证书对应的证书识别信息和公钥维护信息确定第二终端的证书对应的公钥，以及根据第二终端的证书对应的公钥，验证第二终端为通信消息生成的签名。

参阅图 13 所示，本发明实施例提供一种服务器 1300，包括收发器 1301、处理器 1302 和存储器 1303，收发器 1301、处理器 1302 以及存储器 1303 之间通过总线 1304 连接，其中：

收发器 1301，用于接收至少一个终端分别上报的相应终端的证书，以及将公钥维护信息通知给至少一个终端。

存储器 1303，用于存储处理器 1302 执行的程序代码。

处理器 1302, 用于通过存储器 1303 中的程序代码, 执行以下操作: 根据至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息, 公钥维护信息包含预设区域范围内每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息。

本发明实施例中总线 1204 和总线 1304 分别在图 12 和图 13 中以粗线表示, 其它部件之间的连接方式, 仅是进行示意性说明, 并不引以为限。总线 1204 和总线 1304 可以分为地址总线、数据总线、控制总线等。为便于表示, 图 12 和图 13 中仅用一条粗线表示, 但并不表示仅有一根总线或一种类型的总线。

其中, 图 10 中的上报单元、获取单元 1020 和接收单元 1030, 可以由终端 1200 中的收发器 1201 实现, 图 10 中的分析单元 1040 和验证单元 1050 可以由终端中的处理器 1202 实现。图 11 中的接收单元 1110 和发送单元 1130, 可以由服务器 1300 中的收发器 1301 实现, 图 11 中的维护单元 1120, 可以由处理器 1302 实现。

本发明实施例中存储器 1203 和存储器 1303, 用于存储处理器 1202 和处理器 1302 执行的程序代码, 可以是易失性存储器 (英文: volatile memory), 例如随机存取存储器 (英文: random-access memory, 缩写: RAM); 存储器 1203 和存储器 1303 也可以是非易失性存储器 (英文: non-volatile memory), 例如只读存储器 (英文: read-only memory, 缩写: ROM), 快闪存储器 (英文: flash memory), 硬盘 (英文: hard disk drive, 缩写: HDD) 或固态硬盘 (英文: solid-state drive, 缩写: SSD)、或者存储器 1203 和存储器 1303 是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质, 但不限于此。存储器 1203 和存储器 1303 可以是上述存储器的组合。

本发明实施例中处理器 1202 和处理器 1302, 可以是一个中央处理单元 (英文: central processing unit, 简称 CPU)。

本发明实施例中第一终端的证书上报至服务器并从服务器获取公钥维护

信息，使得第一终端在与其他终端进行通信之前及时获取公钥维护信息；第一终端接收第二终端发送的通信信息，通信信息包括第二终端的证书对应的证书识别信息和第二终端为通信消息生成的签名，此时通信消息中不再需要携带第一终端的证书，极大地节省了传输开销；第一终端根据第二终端的证书对应的证书识别信息和公钥维护信息确定第二终端的证书对应的公钥；第一终端根据第二终端的证书对应的公钥，验证第二终端为通信消息生成的签名。服务器接收至少一个终端分别上报的相应终端的证书；服务器根据至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息；服务器将公钥维护信息通知给至少一个终端，使各个终端均能够获取公钥维护信息，保证各个终端间的通信且有效节省了终端间通信的传输开销。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程

和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或

多个流程和 / 或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

显然，本领域的技术人员可以对本发明实施例进行各种改动和变型而不脱离本发明实施例的精神和范围。这样，倘若本发明实施例的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权利要求

1、一种证书通知方法，其特征在于，包括：

第一终端将所述第一终端的证书上报至服务器并从所述服务器获取公钥维护信息，所述公钥维护信息包含预设区域范围内每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息；

所述第一终端接收第二终端发送的通信信息，所述通信信息包括所述第二终端的证书对应的证书识别信息和所述第二终端为所述通信消息生成的签名，所述第二终端为所述通信消息生成的签名为所述第二终端采用所述第二终端的证书对应的私钥对所述通信消息进行签名计算后生成的；

所述第一终端根据所述第二终端的证书对应的证书识别信息和所述公钥维护信息确定所述第二终端的证书对应的公钥；

所述第一终端根据所述第二终端的证书对应的公钥，验证所述第二终端为所述通信消息生成的签名。

2、如权利要求1所述的方法，其特征在于，所述证书识别信息为以下至少一种信息的组合：证书颁发者名称和证书序列号、或者证书名称，或者证书唯一标识。

3、如权利要求1或2所述的方法，其特征在于，第一终端将所述第一终端的证书上报至服务器，包括：

所述第一终端获取到自身的地理位置信息时，将所述地理位置信息和所述第一终端的证书上报至服务器；

或者，所述第一终端检测到新的小区全局标识符 ECGI 时，将所述新的 ECGI 和所述第一终端的证书上报至服务器；

或者，所述第一终端检测到新的跟踪区域码 TAC 时，将所述新的 TAC 和所述第一终端的证书上报至服务器。

4、如权利要求1或2所述的方法，其特征在于，第一终端将所述第一终端的证书上报至服务器，包括：

所述第一终端获取区域配置信息，所述区域配置信息是指以至少一个基站为单位，或以至少一个 TA 为单位，或者根据地理区域进行区域划分的划分结果，每个区域对应一个区域标识；

所述第一终端根据所述区域配置信息确定自身所处区域发生变化时，将所述第一终端的证书和所述第一终端所属区域的区域标识发送至服务器。

5、如权利要求 4 所述的方法，其特征在于，所述第一终端根据所述区域配置信息确定自身所处区域发生变化，包括：

所述第一终端获取到自身的地理位置信息时，根据所述地理位置信息和所述区域配置信息确定自身所属区域发生变化；

或者，所述第一终端检测到新的 ECGI 时，根据所述新的 ECGI 和所述区域配置信息确定自身所属区域发生变化；

或者，所述第一终端检测到新的 TAC 时，根据所述新的跟踪区域码 TAC 和所述区域配置信息确定自身所属区域发生变化。

6、如权利要求 1 或 2 所述的方法，其特征在于，第一终端将所述第一终端的证书上报至服务器，包括：

所述第一终端确定证书更新后需要使用的证书，将所述更新后需要使用的证书上报至所述服务器。

7、如权利要求 1-6 任一项所述的方法，其特征在于，第一终端从所述服务器获取公钥维护信息，包括：

所述第一终端接收所述服务器发送的所述公钥维护信息，

或者，所述第一终端接收所述服务器发送的所述第一终端所属区域的区域标识对应的公钥维护消息和所述第一终端所属区域的区域标识。

8、如权利要求 1-6 所述的方法，其特征在于，第一终端从所述服务器获取公钥维护信息，包括：

所述第一终端接收所述服务器广播的所述公钥维护消息。

或者，所述第一终端接收所述服务器广播的所述第一终端所属区域的区域标识对应的公钥维护消息和所述第一终端所属区域的区域标识。

9、如权利要求 1-8 任一项所述的方法，其特征在于，在第一终端获取公钥维护信息之后，包括：

所述第一终端接收公钥维护更新消息，所述公钥维护更新消息用于更新所述第一终端当前存储的公钥维护信息；

所述第一终端根据所述公钥维护更新消息更新所述当前存储的公钥维护信息。

10、如权利要求 9 所述的方法，其特征在于，所述公钥维护更新消息携带以下至少一种信息的组合：最新公钥维护信息、或者至少一个区域标识和相应区域标识对应的最新公钥维护消息、或者在预设时长内所述公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息以及新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息，或者在预设时长内每个区域标识对应的公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息、新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息和相应的区域标识。

11、一种证书通知方法，其特征在于，包括：

服务器接收至少一个终端分别上报的相应终端的证书；

所述服务器根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息，所述公钥维护信息包含预设区域范围内每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息；

所述服务器将所述公钥维护信息通知给所述至少一个终端。

12、如权利要求 11 所述的方法，其特征在于，所述证书识别信息为以下至少一种信息的组合：证书颁发者名称和证书序列号、或者证书名称，或者证书唯一标识。

13、如权利要求 11 或 12 所述的方法，其特征在于，所述服务器根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书

识别信息更新公钥维护信息，包括：

所述服务器确定第一终端所属区域发生变化时，根据所述第一终端的证书对应的公钥与所述第一终端的证书对应的证书识别信息更新所述第一终端所属区域的区域标识对应的公钥维护信息，或者，更新所述第一终端所属区域的区域标识对应的公钥维护信息以及至少一个所述第一终端所属区域的相邻区域的区域标识分别对应的公钥维护信息，所述第一终端为所述至少一个终端中的任意一个终端。

14、如权利要求 13 所述的方法，其特征在于，所述服务器确定所述第一终端所属区域发生变化，包括：

所述服务器接收所述第一终端上报的所述第一终端所属区域的区域标识；

或者，所述服务器获取区域配置信息，根据所述第一终端上报的地理位置信息和所述区域配置信息确定所述第一终端所属区域发生变化；

或者，所述服务器获取区域配置信息，根据所述第一终端上报的 ECGI 和所述区域配置信息确定所述第一终端所属区域发生变化；

或者，所述服务器获取区域配置信息，根据所述第一终端上报的 TAC 和所述区域配置信息确定所述第一终端所属区域发生变化；

其中，所述区域配置信息是指以至少一个基站为单位，或以至少一个 TA 为单位，或根据地理区域进行区域划分的划分结果，每个区域对应一个区域标识。

15、如权利要求 11-14 任一项所述的方法，其特征在于，所述服务器根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息，包括：

所述服务器确定待分析公钥维护信息集合中包含的第一公钥维护信息超时未针对第二终端的证书对应的公钥与所述第二终端的证书对应的证书识别信息进行更新，则所述服务器将所述第二终端的证书对应的公钥与所述第二终端的证书对应的证书识别信息从所述第一公钥维护信息中删除；

其中，所述待分析公钥维护信息集合中包含至少一个保存第二终端的证

书对应的公钥与所述第二终端的证书对应的证书识别信息的公钥维护信息，所述第一公钥维护信息为所述待分析公钥维护信息集合中的任一条公钥维护信息，所述第二终端为所述至少一个终端中的任意一个终端。

16、如权利要求 11-14 任一项所述的方法，其特征在于，所述服务器根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息，包括：

所述服务器确定第三终端从第一区域移动至第二区域时，确定所述第一区域和所述第二区域分别对应的第一邻区集合和第二邻区集合，所述第一邻区集合包含至少一个所述第一区域的相邻区域的区域标识，所述第二邻区集合包含至少一个所述第二区域的相邻区域的区域标识；

所述服务器确定所述第一邻区集合与所述第二邻区集合的交集，以及待清理集合，所述待清理集合包含所述第一邻区中非所述交集中包含的区域标识；

所述服务器从所述待清理集合中每个区域标识对应的公钥维护信息中，删除所述第三终端的证书对应的公钥与所述第三终端的证书对应的证书识别信息，其中，所述第二终端为所述至少一个终端中的任意一个终端。

17、如权利要求 11-16 任一项所述的方法，其特征在于，所述服务器将所述公钥维护信息通知给所述至少一个终端，包括：

所述服务器发送所述公钥维护信息至所述至少一个终端中的每个终端。或者，所述服务器将所述至少一个终端中的每个终端所属区域的区域标识对应的公钥维护信息和相应终端所属区域的区域标识发送至相应的终端。

18、如权利要求 11-16 任一项所述的方法，其特征在于，所述服务器将所述公钥维护信息通知给所述至少一个终端，包括：

所述服务器广播所述公钥维护消息。

或者，所述服务器广播至少一个区域标识和相应区域标识对应的公钥维护消息。

19、如权利要求 11-18 任一项所述的方法，其特征在于，在所述服务器将

所述公钥维护信息通知给所述至少一个终端之后，还包括：

所述服务器确定并广播公钥维护更新消息，所述公钥维护更新消息用于更新所述至少一个终端中每个终端当前存储的公钥维护信息；

20、如权利要求 19 所述的方法，其特征在于，所述公钥维护更新消息携带以下至少一种信息的组合：最新公钥维护信息、或者至少一个区域标识和相应区域标识对应的最新公钥维护消息、或者在预设时长内所述公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息以及新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息，或者在预设时长内每个区域标识对应的公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息、新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息和相应的区域标识。

21、一种证书通知装置，其特征在于，包括：

上报单元，用于将所述第一终端的证书上报至服务器；

获取单元，用于从所述服务器获取公钥维护信息，所述公钥维护信息包含预设区域范围内每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息；

接收单元，用于接收第二终端发送的通信信息，所述通信信息包括所述第二终端的证书对应的证书识别信息和所述第二终端为所述通信消息生成的签名，所述第二终端为所述通信消息生成的签名为所述第二终端采用所述第二终端的证书对应的私钥对所述通信消息进行签名计算后生成的；

分析单元，用于根据所述第二终端的证书对应的证书识别信息和所述公钥维护信息确定所述第二终端的证书对应的公钥；

验证单元，用于根据所述第二终端的证书对应的公钥，验证所述第二终端为所述通信消息生成的签名。

22、如权利要求 21 所述的装置，其特征在于，所述证书识别信息为以下至少一种信息的组合：证书颁发者名称和证书序列号、或者证书名称，或者

证书唯一标识。

23、如权利要求 21 或 22 所述的装置，其特征在于，将所述第一终端的证书上报至服务器时，所述上报单元，具体用于：

所述第一终端获取到自身的地理位置信息时，将所述地理位置信息和所述第一终端的证书上报至服务器；

或者，所述第一终端检测到新的小区全局标识符 ECGI 时，将所述新的 ECGI 和所述第一终端的证书上报至服务器；

或者，所述第一终端检测到新的跟踪区域码 TAC 时，将所述新的 TAC 和所述第一终端的证书上报至服务器。

24、如权利要求 21 或 22 所述的装置，其特征在于，将所述第一终端的证书上报至服务器时，所述上报单元，具体用于：

获取区域配置信息，所述区域配置信息是指以至少一个基站为单位，或以至少一个 TA 为单位，或者根据地理区域进行区域划分的划分结果，每个区域对应一个区域标识；

根据所述区域配置信息确定自身所处区域发生变化时，将所述第一终端的证书和所述第一终端所属区域的区域标识发送至服务器。

25、如权利要求 24 所述的装置，其特征在于，根据所述区域配置信息确定自身所处区域发生变化时，所述上报单元，还用于：

获取到自身的地理位置信息时，根据所述地理位置信息和所述区域配置信息确定自身所属区域发生变化；

或者，检测到新的 ECGI 时，根据所述新的 ECGI 和所述区域配置信息确定自身所属区域发生变化；

或者，检测到新的 TAC 时，根据所述新的跟踪区域码 TAC 和所述区域配置信息确定自身所属区域发生变化。

26、如权利要求 21 或 22 所述的装置，其特征在于，将所述第一终端的证书上报至服务器，所述上报单元，用于：

确定证书更新后需要使用的证书，将所述更新后需要使用的证书上报至

所述服务器。

27、如权利要求 21-26 任一项所述的装置，其特征在于，从所述服务器获取公钥维护信息，所述获取单元，用于：

接收所述服务器发送的所述公钥维护信息，

或者，接收所述服务器发送的所述第一终端所属区域的区域标识对应的公钥维护消息和所述第一终端所属区域的区域标识。

28、如权利要求 21-26 所述的装置，其特征在于，从所述服务器获取公钥维护信息，所述获取单元，用于：

接收所述服务器广播的所述公钥维护消息。

或者，接收所述服务器广播的所述第一终端所属区域的区域标识对应的公钥维护消息和所述第一终端所属区域的区域标识。

29、如权利要求 21-28 任一项所述的装置，其特征在于，在获取公钥维护信息之后，所述接收单元，还用于所述第一终端接收公钥维护更新消息，所述公钥维护更新消息用于更新所述第一终端当前存储的公钥维护信息；

所述装置还包括：

更新单元，根据所述公钥维护更新消息更新所述当前存储的公钥维护信息。

30、如权利要求 29 所述的装置，其特征在于，所述公钥维护更新消息携带以下至少一种信息的组合：最新公钥维护信息、或者至少一个区域标识和相应区域标识对应的最新公钥维护消息、或者在预设时长内所述公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息以及新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息，或者在预设时长内每个区域标识对应的公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息、新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息和相应的区域标识。

31、一种证书通知装置，其特征在于，包括：

接收单元，用于接收至少一个终端分别上报的相应终端的证书；

维护单元，用于根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息，所述公钥维护信息包含预设区域范围内每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息；

发送单元，用于将所述公钥维护信息通知给所述至少一个终端。

32、如权利要求 31 所述的装置，其特征在于，所述证书识别信息为以下至少一种信息的组合：证书颁发者名称和证书序列号、或者证书名称，或者证书唯一标识。

33、如权利要求 31 或 32 所述的装置，其特征在于，根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息时，所述维护单元，具体用于包括：

确定第一终端所属区域发生变化时，根据所述第一终端的证书对应的公钥与所述第一终端的证书对应的证书识别信息更新所述第一终端所属区域的区域标识对应的公钥维护信息，或者，更新所述第一终端所属区域的区域标识对应的公钥维护信息以及至少一个所述第一终端所属区域的相邻区域的区域标识分别对应的公钥维护信息，所述第一终端为所述至少一个终端中的任意一个终端。

34、如权利要求 33 所述的装置，其特征在于，确定所述第一终端所属区域发生变化时，所述维护单元，还用于：

接收所述第一终端上报的所述第一终端所属区域的区域标识；

或者，获取区域配置信息，根据所述第一终端上报的地理位置信息和所述区域配置信息确定所述第一终端所属区域发生变化；

或者，获取区域配置信息，根据所述第一终端上报的 ECGI 和所述区域配置信息确定所述第一终端所属区域发生变化；

或者，获取区域配置信息，根据所述第一终端上报的 TAC 和所述区域配置信息确定所述第一终端所属区域发生变化；

其中，所述区域配置信息是指以至少一个基站为单位，或以至少一个 TA 为单位，或根据地理区域进行区域划分的划分结果，每个区域对应一个区域标识。

35、如权利要求 31-34 任一项所述的装置，其特征在于，根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息，所述维护单元，还用于：

确定待分析公钥维护信息集合中包含的第一公钥维护信息超时未针对第二终端的证书对应的公钥与所述第二终端的证书对应的证书识别信息进行更新，则所述服务器将所述第二终端的证书对应的公钥与所述第二终端的证书对应的证书识别信息从所述第一公钥维护信息中删除；

其中，所述待分析公钥维护信息集合中包含至少一个保存第二终端的证书对应的公钥与所述第二终端的证书对应的证书识别信息的公钥维护信息，所述第一公钥维护信息为所述待分析公钥维护信息集合中的任一条公钥维护信息，所述第二终端为所述至少一个终端中的任意一个终端。

36、如权利要求 31-34 任一项所述的装置，其特征在于，根据所述至少一个终端中每个终端的证书对应的公钥与相应终端的证书对应的证书识别信息更新公钥维护信息，所述维护单元，还用于：

确定第三终端从第一区域移动至第二区域时，确定所述第一区域和所述第二区域分别对应的第一邻区集合和第二邻区集合，所述第一邻区集合包含至少一个所述第一区域的相邻区域的区域标识，所述第二邻区集合包含至少一个所述第二区域的相邻区域的区域标识；

确定所述第一邻区集合与所述第二邻区集合的交集，以及待清理集合，所述待清理集合包含所述第一邻区中非所述交集中包含的区域标识；

从所述待清理集合中每个区域标识对应的公钥维护信息中，删除所述第三终端的证书对应的公钥与所述第三终端的证书对应的证书识别信息，其中，所述第二终端为所述至少一个终端中的任意一个终端。

37、如权利要求 31-36 任一项所述的装置，其特征在于，将所述公钥维护

信息通知给所述至少一个终端时，所述发送单元，具体用于：

发送所述公钥维护信息至所述至少一个终端中的每个终端。或者，将所述至少一个终端中的每个终端所属区域的区域标识对应的公钥维护信息和相应终端所属区域的区域标识发送至相应的终端。

38、如权利要求 31-36 任一项所述的装置，其特征在于，将所述公钥维护信息通知给所述至少一个终端时，所述发送单元，具体用于：

广播所述公钥维护消息。

或者，广播至少一个区域标识和相应区域标识对应的公钥维护消息。

39、如权利要求 31-38 任一项所述的装置，其特征在于，在将所述公钥维护信息通知给所述至少一个终端之后，所述发送单元还用于：

确定并广播公钥维护更新消息，所述公钥维护更新消息用于更新所述至少一个终端中每个终端当前存储的公钥维护信息。

40、如权利要求 39 所述的装置，其特征在于，所述公钥维护更新消息携带以下至少一种信息的组合：最新公钥维护信息、或者至少一个区域标识和相应区域标识对应的最新公钥维护消息、或者在预设时长内所述公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息以及新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息，或者在预设时长内每个区域标识对应的公钥维护信息中发生公钥更新的终端的证书对应的公钥与相应终端的证书对应的证书识别信息、新增的终端的证书对应的公钥与相应终端的证书对应的证书识别信息和相应的区域标识。

Header 头部	Message body 消息主体	Certificate 证书	Signature 签名
--------------	----------------------	-------------------	-----------------

图 1

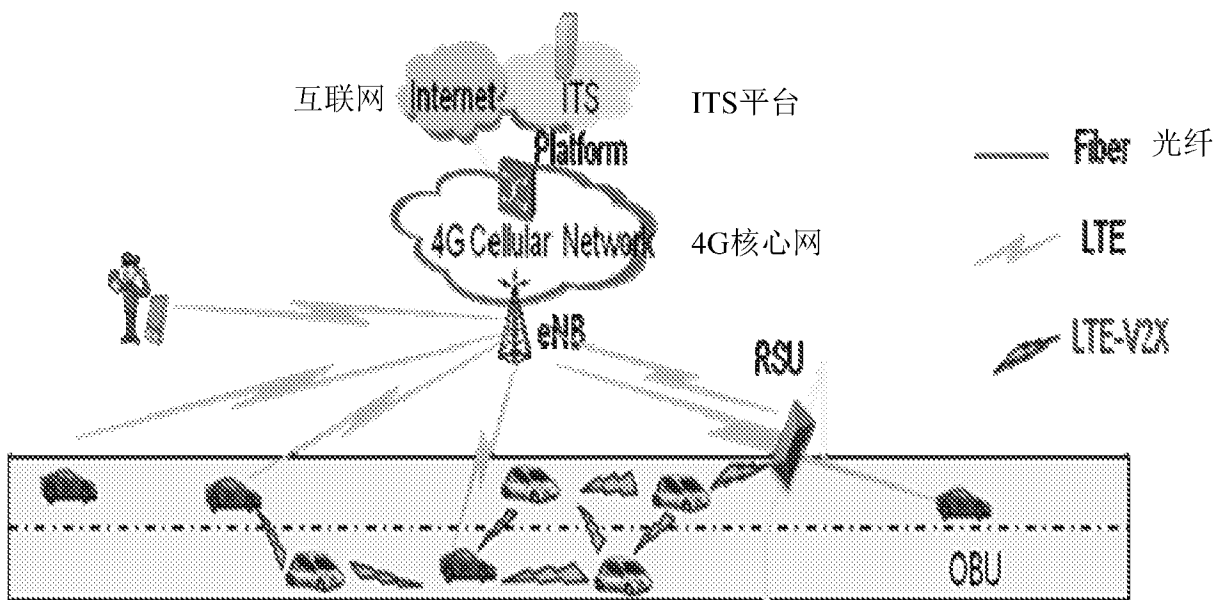


图 2

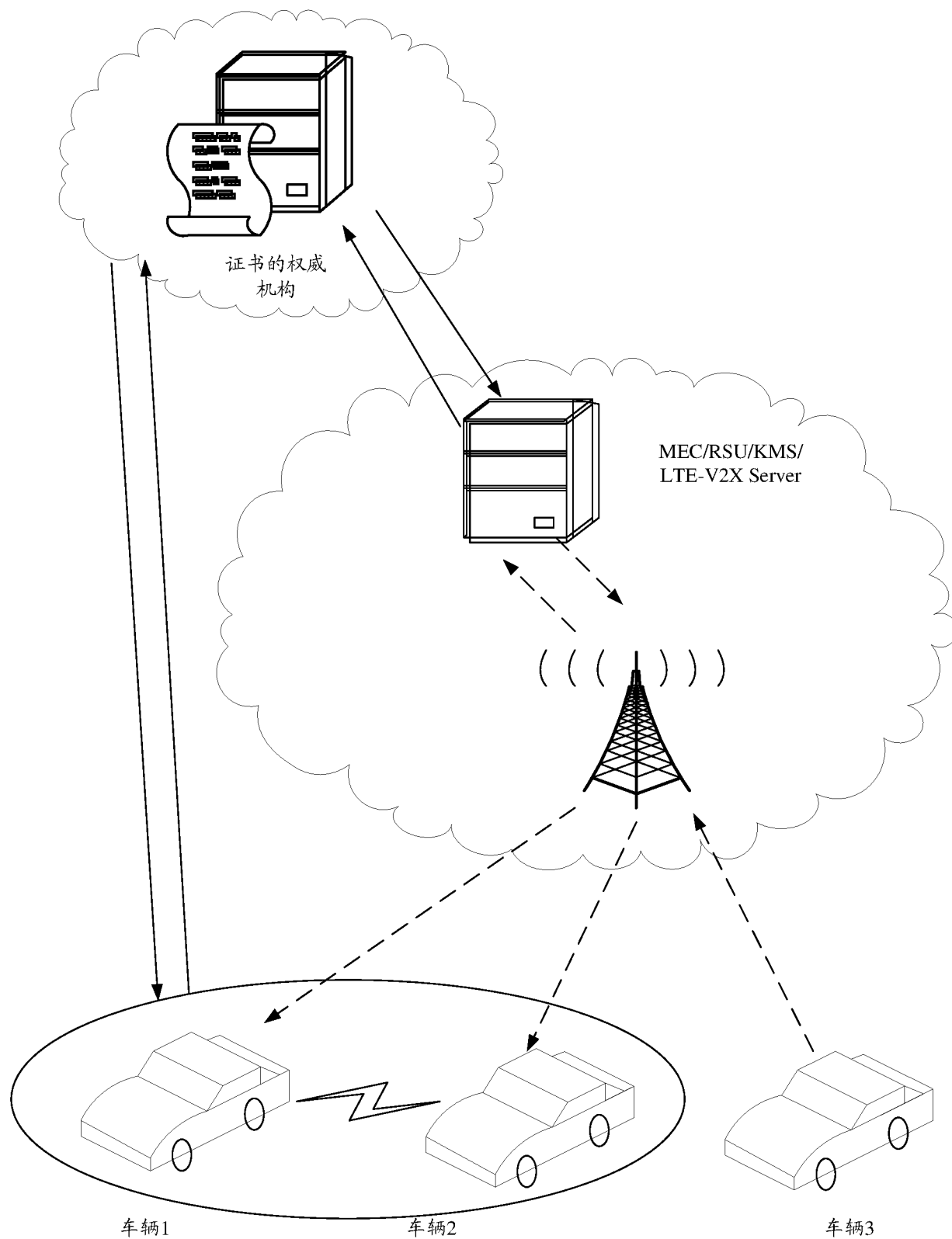


图 3

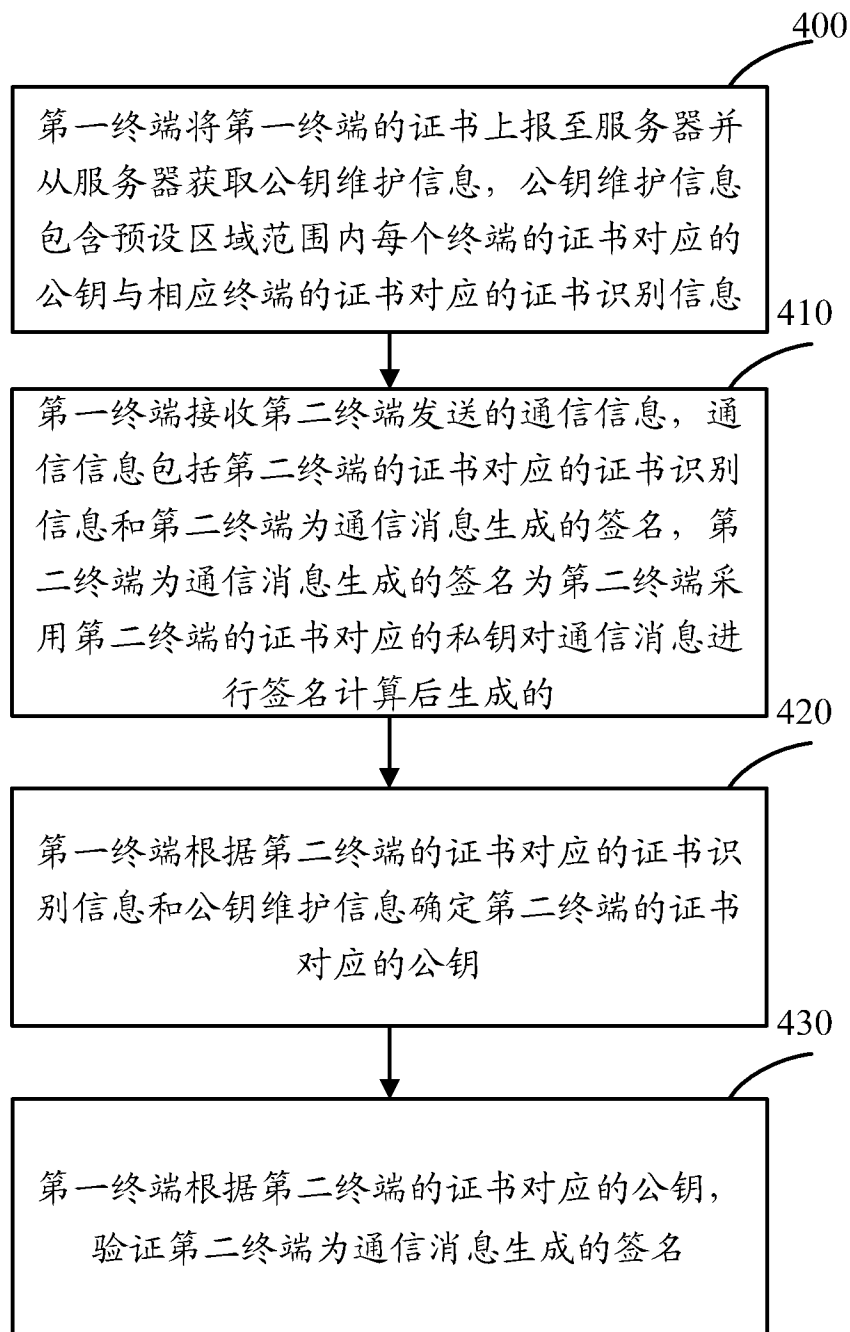


图 4

			7	4	1	
			8	5	2	
			9	6	3	

图 5

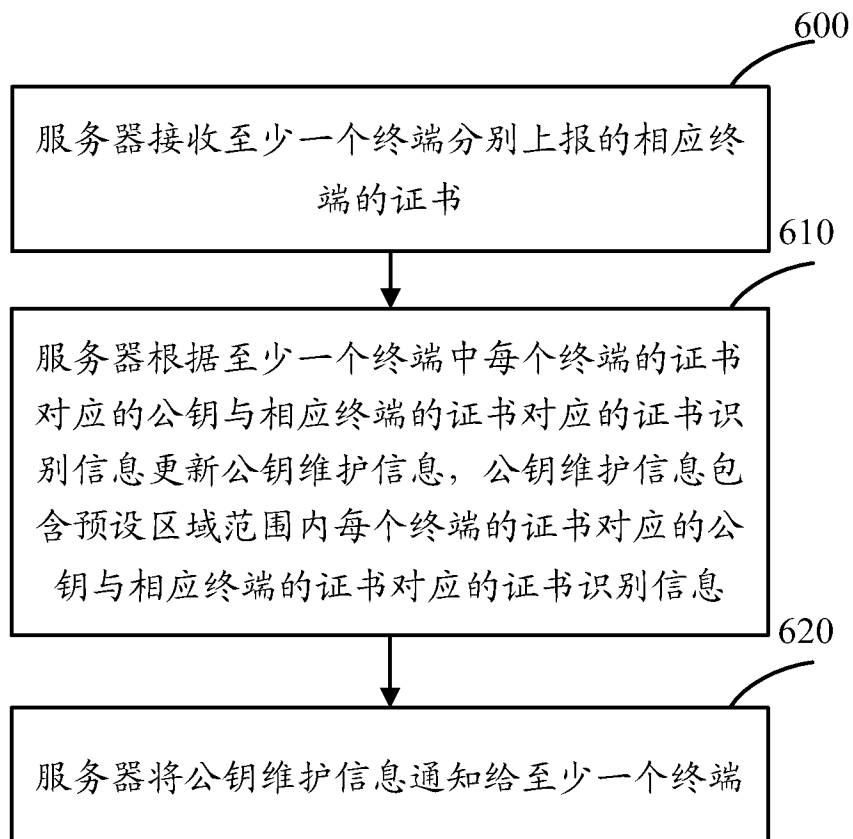


图 6

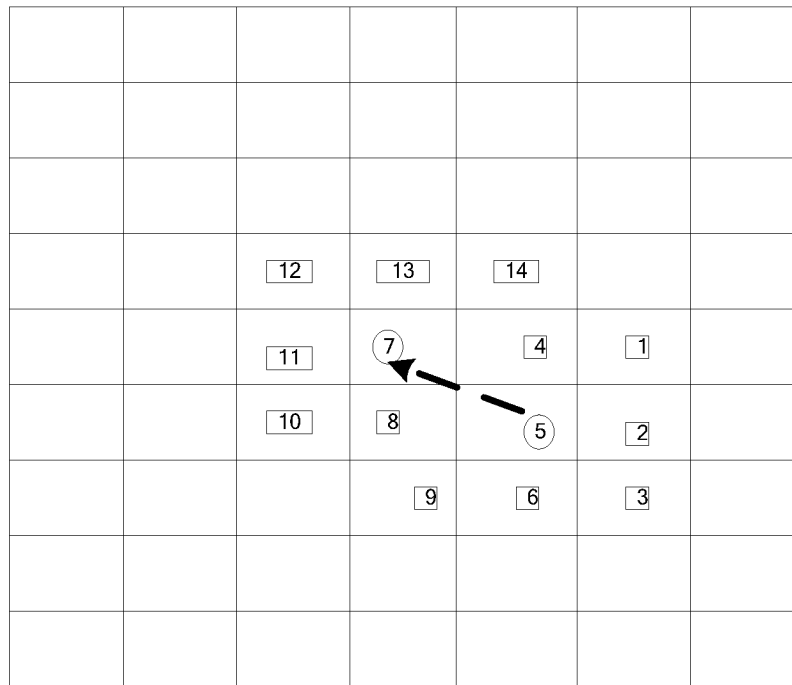


图 7



图 8

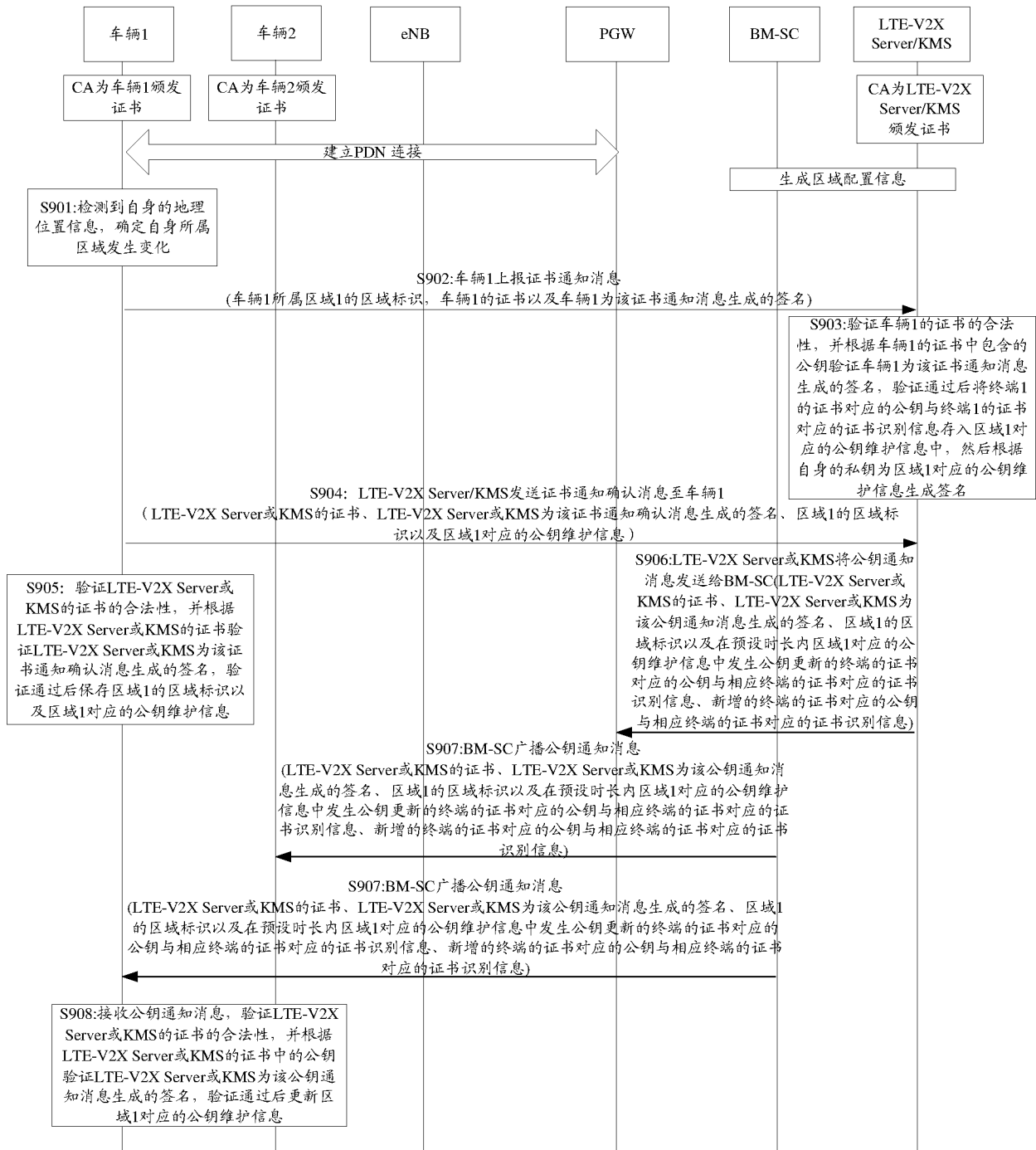


图 9

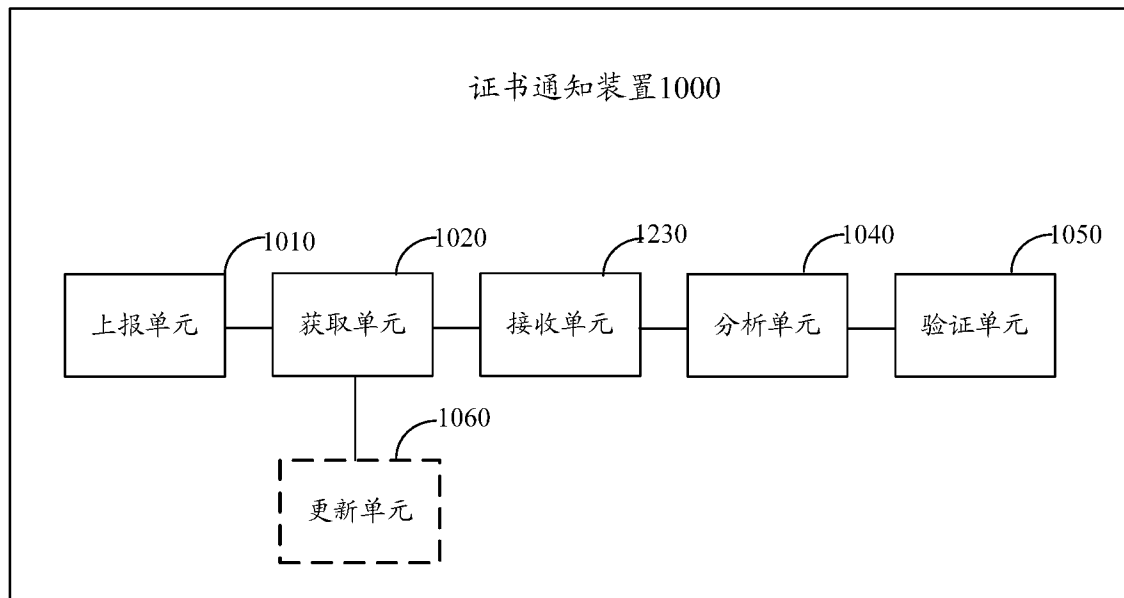


图 10

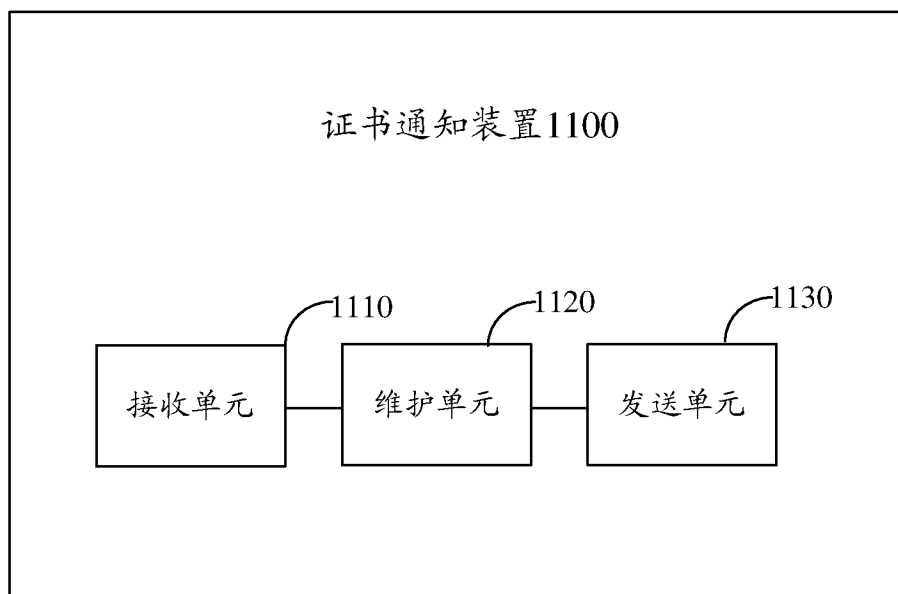


图 11

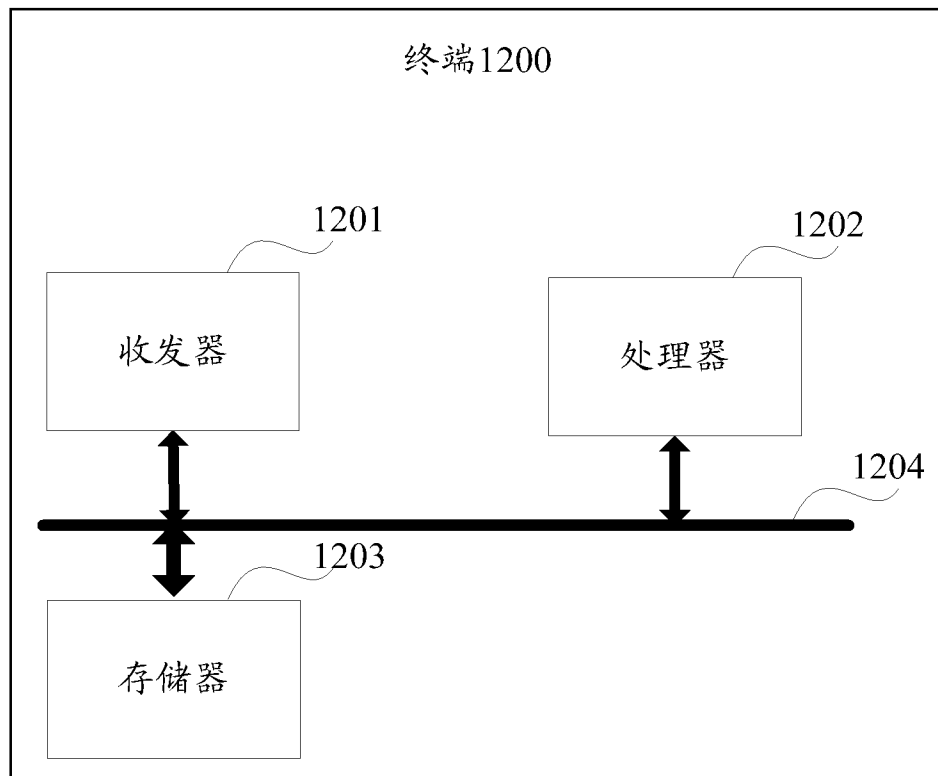


图 12

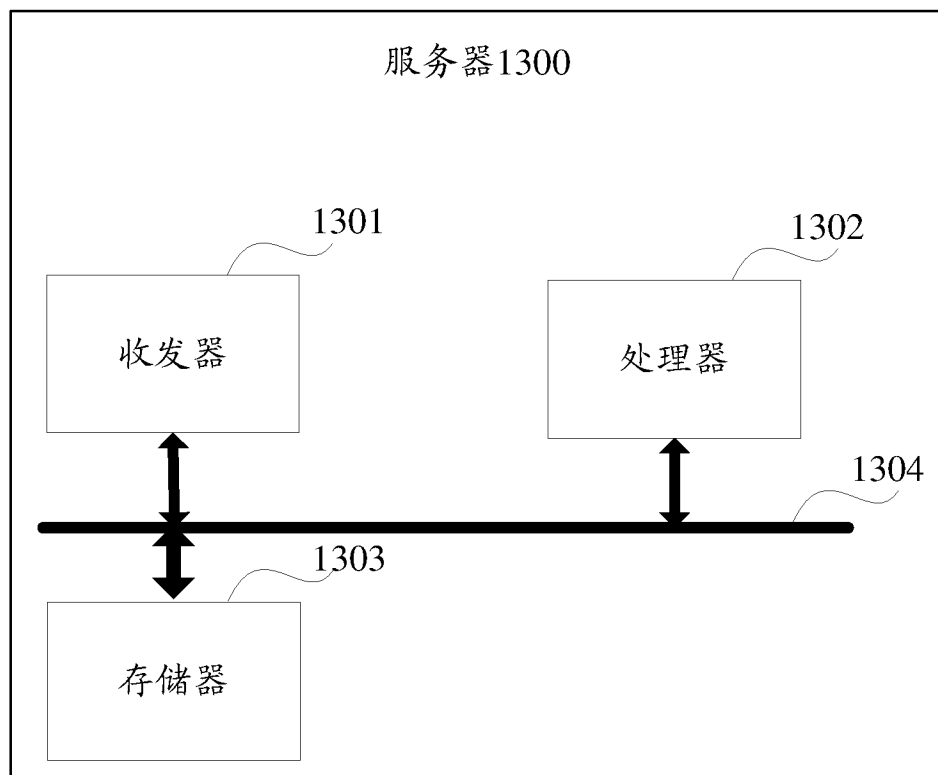


图 13

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/080928**A. CLASSIFICATION OF SUBJECT MATTER**

H04L 9/32(2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L, H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNKI, CNPAT: data amount, no, certificate, overhead, amount, identification, ID, index, server, public key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101860824 A (SHANGHAI HAIJIYE HIGH TECHNOLOGY CO., LTD.), 13 October 2010 (13.10.2010), description, paragraphs [0022]-[0049] and[0068]	1-40
A	CN 101616006 A (ZTE CORP.), 30 December 2009 (30.12.2009), the whole document	1-40
A	US 2015156025 A1 (HUAWEI TECHNOLOGIES CO., LTD.), 04 June 2015 (04.06.2015), the whole document	1-40

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:	
“A” document defining the general state of the art which is not considered to be of particular relevance	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“E” earlier application or patent but published on or after the international filing date	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“O” document referring to an oral disclosure, use, exhibition or other means	“&”document member of the same patent family
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 09January 2017 (09.01.2017)	Date of mailing of the international search report 24January 2017 (24.01.2017)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer LI, Ping Telephone No.:(86-10) 62413398

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/080928

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101860824 A	13 October 2010	CN 101860824 B	12 June 2013
CN 101616006 A	30 December 2009	None	
US 2015156025 A1	04 June 2015	WO 2014019386 A1	06 February 2014
		CN 102801616 A	28 November 2012
		CN 102801616 B	15 April 2015

国际检索报告

国际申请号

PCT/CN2016/080928

A. 主题的分类 H04L 9/32 (2006.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类														
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) H04L, H04W 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) WPI, EPDOC, CNKI, CNPAT: 开销, 数据量, 无, 不, 证书, 识别, 标识, 索引, 服务器, 公钥, overhead, amount, identification, ID, index, server, public key														
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 101860824 A (上海海基业高科技有限公司) 2010年 10月 13日 (2010 - 10 - 13) 说明书第[0022]-[0049]、[0068]段</td> <td>1-40</td> </tr> <tr> <td>A</td> <td>CN 101616006 A (中兴通讯股份有限公司) 2009年 12月 30日 (2009 - 12 - 30) 全文</td> <td>1-40</td> </tr> <tr> <td>A</td> <td>US 2015156025 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 2015年 6月 4日 (2015 - 06 - 04) 全文</td> <td>1-40</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	CN 101860824 A (上海海基业高科技有限公司) 2010年 10月 13日 (2010 - 10 - 13) 说明书第[0022]-[0049]、[0068]段	1-40	A	CN 101616006 A (中兴通讯股份有限公司) 2009年 12月 30日 (2009 - 12 - 30) 全文	1-40	A	US 2015156025 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 2015年 6月 4日 (2015 - 06 - 04) 全文	1-40
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求												
X	CN 101860824 A (上海海基业高科技有限公司) 2010年 10月 13日 (2010 - 10 - 13) 说明书第[0022]-[0049]、[0068]段	1-40												
A	CN 101616006 A (中兴通讯股份有限公司) 2009年 12月 30日 (2009 - 12 - 30) 全文	1-40												
A	US 2015156025 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 2015年 6月 4日 (2015 - 06 - 04) 全文	1-40												
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。														
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件														
国际检索实际完成的日期 2017年 1月 9日		国际检索报告邮寄日期 2017年 1月 24日												
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451		受权官员 李萍 电话号码 (86-10) 62413398												

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/080928

检索报告引用的专利文件				公布日 (年/月/日)		同族专利		公布日 (年/月/日)	
CN	101860824	A	2010年 10月 13日	CN	101860824	B	2013年 6月 12日		
CN	101616006	A	2009年 12月 30日		无				
US	2015156025	A1	2015年 6月 4日	WO	2014019386	A1	2014年 2月 6日		
				CN	102801616	A	2012年 11月 28日		
				CN	102801616	B	2015年 4月 15日		